

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of: Rodney D. Cambridge

Application No.: 09/916,607

Group No.: 2137

Filed: 07/26/2001

Examiner: Pyzocha, Michael J.

For: METHOD AND APPARATUS FOR IMPLEMENTING A HANDHELD SECURITY SYSTEM

**Mail Stop Appeal Briefs – Patents**

**Commissioner for Patents**

**P.O. Box 1450**

**Alexandria, VA 22313-1450**

**TRANSMITTAL OF APPEAL BRIEF  
(PATENT APPLICATION--37 C.F.R. § 41.37)**

1. This brief is in furtherance of the Notice of Appeal, filed in this case on 04/30/2007, and in response to the Notice of Panel Decision from Pre-Appeal Brief Review, mailed 05/21/2007.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	\$500.00
---------------------------	----------

<b>Appeal Brief fee due</b>	<b>\$500.00</b>
-----------------------------	-----------------

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	\$0.00 (previously paid on 07/07/2005)
Extension fee (if any)	\$0.00

<b>TOTAL FEE DUE</b>	<b>\$0.00</b>
----------------------	---------------

6. FEE PAYMENT

Applicant believes that no fees are due in connection with the filing of this paper because the appeal brief fee was paid with a previous submission. However, the Commissioner is authorized to charge any additional fees that may be due (e.g. for any reason including, but not limited to, fee changes, etc.) to Deposit Account No. 50-1351 (Order No. NAIIP312).

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAIIP312).

Date: June 28, 2007

Reg. No.: 41,429  
Tel. No.: 408-971-2573  
Customer No.: 28875

/KEVIN ZILKA/  
Signature of Practitioner  
Kevin J. Zilka  
Zilka-Kotab, PC  
P.O. Box 721120  
San Jose, CA 95172-1120

**PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	)	
	)	
Cambridge, Rodney D.	)	Group Art Unit: 2137
	)	
Application No.: 09/916,607	)	Examiner: Pyzocha, Michael J.
	)	
Filed: 07/26/2001	)	Atty. Docket No.:
	)	NAIIP312/01.048.02
For: METHOD AND APPARATUS FOR	)	
IMPLEMENTING A HANDHELD	)	Date: 06/28/2007
SECURITY SYSTEM	)	

---

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**ATTENTION: Board of Patent Appeals and Interferences**

**APPEAL BRIEF (37 C.F.R. § 41.37)**

This brief is in furtherance of the Notice of Appeal, filed in this case on 04/30/2007, and in response to the Notice of Panel Decision from Pre-Appeal Brief Review, mailed 05/21/2007.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

- I REAL PARTY IN INTEREST
- II RELATED APPEALS AND INTERFERENCES
- III STATUS OF CLAIMS
- IV STATUS OF AMENDMENTS
- V SUMMARY OF CLAIMED SUBJECT MATTER



**I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))**

The real party in interest in this appeal is McAfee, Inc.

## **II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))**

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, prior appeals were noted on 06/02/2005, and on 11/13/2006 in the present application.

A Related Proceedings Appendix is appended hereto.

### **III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))**

#### **A. TOTAL NUMBER OF CLAIMS IN APPLICATION**

Claims in the application are: 1, 3, 5, 6, 10, 14-16, 19, 20, 24-26, 29, 31, and 33-38

#### **B. STATUS OF ALL THE CLAIMS IN APPLICATION**

1. Claims withdrawn from consideration: None
2. Claims pending: 1, 3, 5, 6, 10, 14-16, 19, 20, 24-26, 29, 31, and 33-38
3. Claims allowed: None
4. Claims rejected: 1, 3, 5, 6, 10, 14-16, 19, 20, 24-26, 29, 31, and 33-38
5. Claims cancelled: 2, 4, 7-9, 11-13, 17, 18, 21-23, 27, 28, 30, and 32

#### **C. CLAIMS ON APPEAL**

The claims on appeal are: 1, 3, 5, 6, 10, 14-16, 19, 20, 24-26, 29, 31, and 33-38

See additional status information in the Appendix of Claims.

**IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))**

As to the status of any amendment filed subsequent to the latest final rejection, there are no such amendments after final.



## **V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))**

With respect to a summary of Claim 1, as shown in Figures 1 and 2 et al., a handheld security system comprises a Bluetooth-enabled control unit (e.g. see item 104 of Figure 1, etc.) having a range of communications. The handheld security system further comprises a Bluetooth-enabled device (e.g. see item 108(a) of Figure 1, etc.). Additionally, the device (e.g. see item 108(a) of Figure 1, etc.) is registered with the control unit (e.g. see item 104 of Figure 1, etc.) such that the device cooperates with the control unit using Bluetooth communications to determine when the device is within the range of communications (e.g. see item 112 of Figure 1, etc.) of the control unit. Furthermore, when it is determined that the device (e.g. see item 108(a) of Figure 1, etc.) is within the range of communications (e.g. see item 112 of Figure 1, etc.) of the control unit (e.g. see item 104 of Figure 1, etc.), the device is functional, and when it is determined that the device is not within the range of communications of the control unit (e.g. see item 112 of Figure 2, etc.), the device is at least partially non-functional.

Further still, the device (e.g. see item 108(a) of Figure 1, etc.) is configured to periodically send an identifying signal to the control unit (e.g. see item 104 of Figure 1, etc.) and the control unit is configured to send a return signal to the device when the identifying signal is received by the control unit. In addition, when the device (e.g. see item 108(a) of Figure 2, etc.) is at least partially non-functional in a situation where it is determined that the device is not within the range of communications (e.g. see item 112 of Figure 2, etc.) of the control unit (e.g. see item 104 of Figure 2, etc.), the device is configured to continue periodically sending the identifying signal to the control unit.

Further, the control unit (e.g. see item 104 of Figure 2, etc.) is configured to produce an alert when it is determined that the device (e.g. see item 108(a) of Figure 2, etc.) is not within the range of communications (e.g. see item 112 of Figure 2, etc.) of the control. Additionally, the control unit (e.g. see item 104 of Figure 2, etc.) includes a control unit display, the control unit display being configured to display information associated with the device when it is determined that the device is not within the range of communications of the control unit.

Furthermore, the device (e.g. see item 108(a) of Figure 2, etc.) includes a device display, the device display being configured to display information associated with the control unit (e.g. see item 104 of Figure 2, etc.) when it is determined that the device is not within the range of communications of the control unit. Further still, the device (e.g. see item 108(a) of Figure 2, etc.) is configured to periodically send the identifying signal utilizing a period of time which is configured based on movements of an owner. See, for example, page 3, lines 17-27; page 3, line 29-page 4, line 6; page 12, lines 20-26; and page 12, line 29-page 13, line 2 et al.

With respect to a summary of Claim 10, as shown in Figures 1, 3A, and 3B et al., a method for executing a security protocol for a first Bluetooth-enabled device (e.g. see item 108(a) of Figure 1, etc.) with respect to a second Bluetooth-enabled device (e.g. see item 104 of Figure 1, etc.) is provided. In use, a first Bluetooth transmission signal is periodically emitted from the first Bluetooth-enabled device (e.g. see item 316 of Figure 3A, etc.). Additionally, it is determined if a second Bluetooth transmission signal is received from the second Bluetooth-enabled device (e.g. see item 320 of Figure 3A, etc.). Further, the first Bluetooth-enabled device is locked out to at least partially prevent the first Bluetooth-enabled device from functioning if it is determined that the second Bluetooth transmission signal is not received (e.g. see item 324 of Figure 3A, etc.).

Further still, the first Bluetooth-enabled device periodically emits the first Bluetooth transmission signal while being locked out in a situation where it is determined that the second Bluetooth transmission signal is not received (e.g. see item 332 of Figure 3B, etc.). Additionally, the second Bluetooth-enabled device is configured to produce an alert when it is determined that the second Bluetooth transmission signal is not received (e.g. see item 328 of Figure 3A, etc.). Furthermore, the second Bluetooth-enabled device includes a second Bluetooth-enabled device display, the second Bluetooth-enabled device display being configured to display information associated with the first Bluetooth-enabled device when the first Bluetooth-enabled device is locked out (e.g. see item 328 of Figure 3A, etc.).

Also, the first Bluetooth-enabled device includes a first Bluetooth-enabled device display, the first Bluetooth-enabled device display being configured to display information associated with the second Bluetooth-enabled device when the first Bluetooth-enabled device is locked out (e.g.

see item 324 of Figure 3A, etc.). In addition, the first Bluetooth-enabled device is configured to periodically emit the first Bluetooth transmission signal utilizing a period of time which is configured based on movements of an owner (e.g. see item 316 of Figure 3A, etc.). See, for example, page 3, line 29-page 4, line 6; page 4, lines 20-27; page 12, lines 20-26; and page 12, line 29-page 13, line 2 et al.

With respect to a summary of Claim 16, as shown in Figures 1, 3A, and 3B et al., a method for executing a security protocol with respect to at least a first Bluetooth-enabled device (e.g. see item 104 of Figure 1, etc.) and a second Bluetooth-enabled device (e.g. see item 108(a) of Figure 1, etc.) is provided. In use, it is determined when a first Bluetooth transmission signal is received from the second Bluetooth-enabled device (e.g. see item 320 of Figure 3A, etc.). The second Bluetooth-enabled device automatically and periodically emits the first Bluetooth transmission signal (e.g. see item 316 of Figure 3A, etc.). Additionally, a second Bluetooth transmission signal is emitted when it is determined that the first Bluetooth transmission signal is received from the second Bluetooth-enabled device (e.g. see item 316 of Figure 3A, etc.).

Further, an alarm is generated to indicate that the second Bluetooth-enabled device is not within a communications range of the first Bluetooth-enabled device when it is determined that the first Bluetooth transmission signal is not received from the second Bluetooth-enabled device (e.g. see item 324 of Figure 3A, etc.). Additionally, after the generation of the alarm, the second Bluetooth-enabled device is configured to continue periodically emit the first Bluetooth transmission signal to the first Bluetooth-enabled device in a situation where it is determined that the first Bluetooth-enabled device is not within the range of communications of the second Bluetooth-enabled device (e.g. see item 336 of Figure 3B, etc.).

Further, the second Bluetooth-enabled device includes a second Bluetooth-enabled device display, the second Bluetooth-enabled device display being configured to display information associated with the first Bluetooth-enabled device when it is determined that the first Bluetooth-enabled device is not within the range of communications of the second Bluetooth-enabled device (e.g. see item 324 of Figure 3A, etc.). Further still, the first Bluetooth-enabled device includes a first Bluetooth-enabled device display, the first Bluetooth-enabled device display being configured to display information associated with the second Bluetooth-enabled device

when it is determined that the first Bluetooth-enabled device is not within the range of communications of the second Bluetooth-enabled device (e.g. see item 328 of Figure 3A, etc.). Additionally, the second Bluetooth-enabled device is configured to periodically emit the first Bluetooth transmission signal utilizing a period of time which is configured based on movements of an owner (e.g. see item 316 of Figure 3A, etc.). See, for example, page 5, lines 13-24; page 12, lines 20-26; and page 12, line 29-page 13, line 2 et al.

With respect to a summary of Claim 20, as shown in Figures 3A, 3B, 4 and 6 et al., a first device (e.g. see item 608 of Figure 6, etc.) comprises a Bluetooth-enabled mechanism. In addition, the first device comprises computer code that causes the Bluetooth-enabled mechanism (e.g. see item 672 of Figure 6, etc.) to periodically emit a first Bluetooth transmission signal (e.g. see item 404 of Figure 4, etc.). Further, the first device comprises computer code that causes the Bluetooth-enabled mechanism to receive a second Bluetooth transmission signal from a second Bluetooth-enabled device (e.g. see item 604 of Figure 6, etc.). Further still, the first device comprises computer code for determining when the second Bluetooth transmission signal is received (e.g. see item 408 of Figure 4, etc.).

Additionally, the first device comprises computer code for locking out the first device to at least partially prevent the first device from being operational when it is determined that the second Bluetooth transmission signal is not received (e.g. see item 416 of Figure 4, etc.). The Bluetooth-enabled mechanism periodically emits the first Bluetooth transmission signal while the first device is locked out in a situation where it is determined that the second Bluetooth transmission signal is not received (e.g. see item 332 of Figure 3B, etc.). Furthermore, the first device comprises a processor (e.g. see item 662 of Figure 6, etc.) for executing the computer codes, and a computer-readable medium (e.g. see items 664, 666, 668 of Figure 6, etc.) that stores the computer codes.

In addition, the second Bluetooth-enabled device is configured to produce an alert when it is determined that the second Bluetooth transmission signal is not received (e.g. see item 328 of Figure 3A, etc.). Also, the second Bluetooth-enabled device includes a second Bluetooth-enabled device display (e.g. see item 620 of Figure 6, etc.), the second Bluetooth-enabled device display being configured to display information associated with the first device when the first

device is locked out (e.g. see item 328 of Figure 3A, etc.). Furthermore, the first device includes a first device display (e.g. see item 670 of Figure 6, etc.), the first device display being configured to display information associated with the second Bluetooth-enabled device when the first device is locked out (e.g. see item 324 of Figure 3A, etc.). Additionally, the Bluetooth-enabled mechanism is configured to periodically emit the first Bluetooth transmission signal utilizing a period of time which is configured based on movements of an owner (e.g. see item 316 of Figure 3A, etc.). See, for example, page 4, lines 20-27; page 12, lines 20-26; and page 12, line 29-page 13, line 2 et al.

With respect to a summary of Claim 26, as shown in Figures 3A, 4, and 6 et al., a first device (e.g. see item 604 of Figure 6, etc.) comprises a Bluetooth-enabled mechanism (e.g. see item 622 of Figure 6, etc.), the Bluetooth-enabled mechanism being configured to receive a first Bluetooth transmission signal from a second device (e.g. see item 608 of Figure 6, etc.) that periodically emits the first Bluetooth transmission signal (e.g. see item 404 of Figure 4, etc.). In addition, the first device comprises computer code for determining when a first Bluetooth transmission signal is received. Further, the first device comprises computer code for causing the Bluetooth-enabled mechanism (e.g. see item 622 of Figure 6, etc.) to emit a second Bluetooth transmission signal when it is determined that the first Bluetooth transmission signal is received (e.g. see item 408 of Figure 4, etc.).

Further still, the first device comprises computer code for generating an alarm to indicate that the second device is not within a communications range of the first device when it is determined that the first Bluetooth transmission signal is not received (e.g. see item 328 of Figure 3A, etc.). After the generation of the alarm, the second device is configured to continue periodically emitting the first Bluetooth transmission signal in a situation where it is determined that the first device is not within the range of communications of the second device (e.g. see item 316 of Figure 3A, etc.). Also, the first device comprises a processor (e.g. see item 612 of Figure 6, etc.) that executes the computer codes. The first device also comprises a computer-readable medium that stores the computer codes (e.g. see items 614, 616, 618 of Figure 6, etc.).

Additionally, the second device includes a second device display (e.g. see item 670 of Figure 6, etc.), the second device display being configured to display information associated with the first

device when it is determined that the first device is not within the range of communications of the second device (e.g. see item 324 of Figure 3A, etc.). Furthermore, the first device includes a first device display (e.g. see item 620 of Figure 6, etc.), the first device display being configured to display information associated with the second device when it is determined that the first is not within the range of communications of the second device (e.g. see item 328 of Figure 3A, etc.). In addition, the second device is configured to periodically emit the first Bluetooth transmission signal utilizing a period of time configured which is based on movements of an owner (e.g. see item 316 of Figure 3A, etc.). See, for example, page 5, lines 13-24; page 12, lines 20-26; and page 12, line 29-page 13, line 2 et al.

With respect to a summary of Claim 29, as shown in Figures 3A, 3B, and 6 et al., a handheld security system comprises a WiFi-enabled control unit (e.g. see item 604 of Figure 6, etc.) having a range of communications. In addition, the handheld security system comprises a WiFi-enabled device (e.g. see item 608 of Figure 6, etc.). The device is registered with the control unit (e.g. see item 304 of Figure 3A, etc.) such that the device cooperates with the control unit using WiFi communications to determine when the device is within the range of communications of the control unit. Further, when it is determined that the device is within the range of communications of the control unit, the device is functional (e.g. see item 308 of Figure 3A, etc.), and when it is determined that the device is not within the range of communications of the control unit, the device is at least partially non-functional (e.g. see item 324 of Figure 3A, etc.).

Furthermore, the device is configured to periodically send an identifying signal to the control unit and the control unit is configured to send a return signal to the device when the identifying signal is received by the control unit (e.g. see item 316 of Figure 3A, etc.). Additionally, when the device is at least partially non-functional in a situation where it is determined that the device is not within the range of communications of the control unit, the device is configured to continue periodically sending the identifying signal to the control unit (e.g. see item 336 of Figure 3B, etc.). Further still, the control unit is configured to produce an alert when it is determined that the device is not within the range of communications of the control unit (e.g. see item 328 of Figure 3B, etc.).

In addition, the control unit includes a control unit display (e.g. see item 620 of Figure 6, etc.), the control unit display being configured to display information associated with the device when it is determined that the device is not within the range of communications of the control unit. Additionally, the device includes a device display (e.g. see item 670 of Figure 6, etc.), where the device display is configured to display information associated with the control unit when it is determined that the device is not within the range of communications of the control unit. Further, the device is configured to periodically send the identifying signal utilizing a period of time which is configured based on movements of an owner (e.g. see item 316 of Figure 3A, etc.). See, for example, page 3, line 17 – page 4, line 1; page 12, lines 20-26; and page 12, line 29-page 13, line 2 et al.

Of course, the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

**VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))**

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1, 3, 5-6, 10, 15-16, 19-20, 25-26, and 34-38 under 35 U.S.C. 103(a) as being unpatentable over Doub (U.S. Patent No. 6,594,762), in view of Lunsford et al. (U.S. Patent No. 6,614,350), and in further view of Logan (U.S. Patent No. 6,631,271).

Issue # 2: The Examiner has rejected Claims 14 and 24 under 35 U.S.C. 103(a) as being unpatentable over Doub, in view of Lunsford et al., in view of Logan, and in further view of Parker (U.S. Patent Publication No. 2002/0078393).

Issue # 3: The Examiner has rejected Claims 29, 31, and 33 under 35 U.S.C. 103(a) as being unpatentable over Doub, in view of Lunsford et al., in view of Logan, and in further view of Lenz (U.S. Patent Publication No. 2001/0053947).



## VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

### Issue # 1:

The Examiner has rejected Claims 1, 3, 5-6, 10, 15-16, 19-20, 25-26, and 34-38 under 35 U.S.C. 103(a) as being unpatentable over Doub (U.S. Patent No. 6,594,762), in view of Lunsford et al. (U.S. Patent No. 6,614,350), and in further view of Logan (U.S. Patent No. 6,631,271).

#### *Group #1: Claims 1, 3, 5, 10, 15-16, 19-20, 25-26, and 34-38*

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the first element of the *prima facie* case of obviousness and, in particular, the obviousness of combining the Doub and Lunsford references, the Examiner has argued that it would have been obvious to combine Doub with Lunsford "to include the Bluetooth alerting of Lunsford et al. in the system of Doub," and that the "[m]otivation to do so would have been to deter the theft and prevent inadvertent abandonment of various portable devices (see Lunsford et al. column 2 lines 37-47)." To the contrary, appellant respectfully asserts that it would not have been obvious to combine the teachings of the Doub and Lunsford references, especially in view of the vast evidence to the contrary.

If a proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). Thus, the claimed combination cannot change the principle of operation of the primary reference or render the reference inoperable for its intended purpose. See MPEP § 2143.01.

In particular, in the Office Action dated 08/18/2006, the Examiner admitted that “Doub clearly and expressly teaches a handheld security system which is maintained between ‘an electronic device and a remote device’ (abstract line 1).” The Examiner further noted that “[t]he entire disclosure relates to a system in which one device is controlled by one control unit (e.g. Col 1, line 46 to Col 2, line 16; Fig 1).” Additionally, the Examiner admitted that “[n]ot only is there no disclosure that a device is registered with more than one control unit, such teaching would appear to be logically inconsistent with Doub as Doub’s control unit would be inoperable to control the device if the device were...registered with other control units seeking to control the device” ( See page 10 of the Office Action dated 08/18/2006-emphasis added).

However, appellant respectfully asserts that Lunsford teaches “a method and system for effecting a security system upon multiple devices” and that “[t]he invention provides for multiple devices to respond as authorized members of a security web such that each device acts as a co-monitoring device within the web” (see Col. 2, lines 37-41; and Figures 1-4 – emphasis added). Lunsford further teaches that “each device periodically polls for the presence of all the other devices in the piconet and if the signal from any device is not detected by any other device in the piconet then all devices sound an alarm” (Col. 8, lines 42-45 – emphasis added). Thus, because Lunsford clearly teaches multiple devices where each device polls all other devices, the devices in Lunsford are clearly registered with other devices.

Therefore, since Doub discloses a device that is only registered with a single control unit, and the control unit of Doub would be inoperable to control the device if the device were registered to more than one control unit, as admitted by the Examiner, it is clear that modifying the device of Doub according to the system of Lunsford, in which a device is registered with multiple other devices, would render the invention of Doub unsatisfactory for its intended purpose. To emphasize, because the Examiner has admitted that “Doub’s control unit would be inoperable to

control the device if the device were...registered with other control units seeking to control the device” (emphasis added), and Lunsford teaches multiple devices polling other devices, the Examiner’s proposed combination of the Doub and Lunsford reference is improper under *In re Gordon*.

Additionally, appellant respectfully asserts that the third element of the *prima facie* case of obviousness has also not been met by the prior art excerpts relied on by the Examiner. For example, with respect to the independent claims, the Examiner has relied on Col. 7, lines 9-15; and Col. 8 lines 38-49 from Lunsford to make a prior art showing of appellant’s claimed technique “wherein the control unit includes a control unit display, the control unit display being configured to display information associated with the device when it is determined that the device is not within the range of communications of the control unit” (see this or similar, but not necessarily identical language in the independent claims).

Appellant respectfully asserts that Col. 7, lines 9-15 from Lunsford, as relied on by the Examiner, merely teaches that “upon the determination of a non-authorized loss of proximity, an event is initiated upon at least one device in the security web” and that “[t]he event initiated may vary widely with examples being the activation of audio and visual alarms, the activation and deactivation of user pre-determined devices, and the transmission of communications to a device outside of the security web” (Col. 7, lines 9-15 — emphasis added).

However, only generally disclosing that visual alarms may be initiated upon the loss of proximity of a device, as in Lunsford, in no way specifically suggests that “the control unit includes a control unit display, the control unit display being configured to display information associated with the device when it is determined that the device is not within the range of communications of the control unit” (see at least substantially the same subject matter in each of the independent claims—emphasis added), as claimed by appellant. Simply indicating that a visual alarm may be initiated, as in Lunsford, simply fails to meet “display[ing] information associated with the device” via “a control unit display” (see at least substantially the same subject matter in each of the independent claims—emphasis added), as claimed by appellant.

Additionally, Col. 8, lines 45-49 from Lunsford, as relied on by the Examiner, simply teaches that “any device which loses contact with all other devices of the piconet displays the owners name, address, and telephone number and then locks itself from further use until such time as a password is entered into the device” (emphasis added).

However, displaying the owner’s name, address, and telephone number on the device which has lost contact with all other devices, as in Lunsford, in no way suggests that “the control unit includes a control unit display, the control unit display being configured to display information associated with the device when it is determined that the device is not within the range of communications of the control unit” (see at least substantially the same subject matter in each of the independent claims-emphasis added), as claimed by appellant. Clearly, displaying the owner’s information on the device which has lost contact, as in Lunsford, fails to suggest “display[ing] information associated with the device” via “a control unit display” (see at least substantially the same subject matter in each of the independent claims-emphasis added), as claimed by appellant.

In addition, with respect to the independent claims, the Examiner has again relied on Col. 7, lines 9-15 and Col. 8, lines 38-49 in Lunsford to make a prior art showing of appellant’s claimed technique “wherein the device includes a device display, the device display being configured to display information associated with the control unit when it is determined that the device is not within the range of communications of the control unit” (see this or similar, but not necessarily identical language in the independent claims).

Appellant respectfully asserts that, as argued above, the excerpts relied on by the Examiner only generally disclose that visual alarms may be initiated upon the loss of proximity of a device and that the owner’s name, address, and telephone number are displayed on the device which has lost contact with all other devices. Clearly, only generally disclosing visual alarms, along with displaying information on the device which has lost contact with all other devices, as in Lunsford, fails to meet appellant’s claimed technique “wherein the device includes a device display, the device display being configured to display information associated with the control unit when it is determined that the device is not within the range of communications of the

control unit” (see at least substantially the same subject matter in each of the independent claims-emphasis added), as claimed.

Further, with respect to the independent claims, the Examiner has relied on Col. 2, lines 30-63; and Col. 6, lines 41-53 from Logan to make a prior art showing of appellant’s claimed technique “wherein the device is configured to periodically send the identifying signal utilizing a period of time which is configured based on movements of an owner” (see this or similar, but not necessarily identical language in the independent claims).

Appellant respectfully asserts that the excerpts relied on by the Examiner merely teach that “Blue Tooth chips could be integrated into a small device (here called a “badge”) whose prime function is to indicate position and which can be...placed on or near stationary devices, such as the Palm docking station, or the cell phone recharger, with which Bluetooth devices or things bearing other Bluetooth badges could link to at times” (Col. 6, lines 47-53 - emphasis added). In addition, the excerpts relied on by the Examiner teach that “[a]lthough the Bluetooth chips in these devices may be primarily intended for different functions, they can play a useful role in the position monitoring and notification system contemplated by the present invention” (Col. 2, lines 59-62 -- emphasis added).

However, using Blue Tooth chips to indicate position and for position monitoring, as in Logan, fails to even suggest “a period of time which is configured based on movements of an owner,” let alone that “the device is configured to periodically send the identifying signal utilizing a period of time which is configured based on movements of an owner” (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

*Group #2: Claim 6*

With respect to Claim 6, the Examiner has relied on Col. 3, line 19 to Col. 4, line 63 from Doub, and Col. 8, lines 38-49 from Lunsford to make a prior art showing of appellant's claimed technique "wherein the device is exclusively registered with the control unit."

Appellant respectfully asserts that the excerpt from Doub relied upon by the Examiner merely discloses that "during an initial set-up procedure, the user may input a password or other data into the electronic device 100 and the remote device 110 to create the first authentication code" where "the electronic device 100 checks the reply signal for the data or password provided by the user" (emphasis added). Further, Doub teaches that "[i]f the reply signal does not include the correct first authentication code, the display controller 210 will not enable the display 115."

However, merely teaching that the user inputs a password into the electronic device and remote device and that the electronic device checks the reply signal for the password before enabling the display fails to even suggest a technique "wherein the device is exclusively registered with the control unit" (emphasis added), as claimed. Clearly, Doub's teachings that the electronic device enables the display if the reply signal contains the correct password fails to even suggest a technique "wherein the device is exclusively registered with the control unit" (emphasis added), as claimed by appellant.

Further, appellant respectfully asserts that the excerpt from Lunsford relied upon by the Examiner merely teaches that "multiple Bluetooth enabled portable information devices... are communicatively connected to every other device within a Bluetooth piconet," that "[e]ach device periodically polls for the presence of all the other devices in the piconet," and that "if the signal from any device is not detected by any other device in the piconet then all devices sound an alarm" (Col. 8, lines 38-45 – emphasis added). Further, Lunsford teaches that "any device which loses contact with all other devices of the piconet displays the owners name, address, and telephone number and then locks itself from further use" (Col. 8, lines 45-49).

However, polling for the presence of all other devices in a network and sounding an alarm if any device is not detected by any other device, in addition to displaying owner information when a device loses contact with all other devices, does not teach a technique "wherein the device is exclusively registered with the control unit" (emphasis added), as claimed by appellant. In fact,

teaching that a device polls for the presence of all other devices in a network, as in Lunsford, *teaches away* from a technique “wherein the device is exclusively registered with the control unit” (emphasis added), as claimed by appellant. A *prima facie* case of obviousness may also be rebutted by showing that the art, in any material respect, teaches away from the claimed invention. *In re Geisler*, 116 F.3d 1465, 1471, 43 USPQ2d 1362, 1366 (Fed. Cir. 1997).

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Issue # 2:

The Examiner has rejected Claims 14 and 24 under 35 U.S.C. 103(a) as being unpatentable over Doub, in view of Lunsford et al., in view of Logan, and in further view of Parker (U.S. Patent Publication No. 2002/0078393).

*Group #1: Claims 14 and 24*

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued with respect to Issue #1, Group #1.

Issue # 3:

Issue # 3: The Examiner has rejected Claims 29, 31, and 33 under 35 U.S.C. 103(a) as being unpatentable over Doub, in view of Lunsford et al., in view of Logan, and in further view of Lenz (U.S. Patent Publication No. 2001/0053947).

*Group #1: Claims 29, 31, and 33*

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine

reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the first element of the *prima facie* case of obviousness and, in particular, the obviousness of combining the Doub and Lunsford references, the Examiner has argued that it would have been obvious to combine Doub with Lunsford "to include the Bluetooth alerting of Lunsford et al. in the system of Doub," and that the "[m]otivation to do so would have been to deter the theft and prevent inadvertent abandonment of various portable devices (see Lunsford et al. Col. 2, lines 37-47)." To the contrary, appellant respectfully asserts that it would not have been obvious to combine the teachings of the Doub and Lunsford references, especially in view of the vast evidence to the contrary.

If a proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). Thus, the claimed combination cannot change the principle of operation of the primary reference or render the reference inoperable for its intended purpose. See MPEP § 2143.01.

In particular, in the Office Action dated 08/18/2006, the Examiner admitted that "Doub clearly and expressly teaches a handheld security system which is maintained between 'an electronic device and a remote device' (abstract line 1)." The Examiner further noted that "[t]he entire disclosure relates to a system in which one device is controlled by one control unit (e.g. Col 1, line 46 to Col 2, line 16; Fig 1)." Additionally, the Examiner admitted that "[n]ot only is there no disclosure that a device is registered with more than one control unit, such teaching would appear to be logically inconsistent with Doub as Doub's control unit would be inoperable to control the device if the device were...registered with other control units seeking to control the device" ( See page 10 of the Office Action dated 08/18/2006-emphasis added).



However, appellant respectfully asserts that Lunsford teaches “a method and system for effecting a security system upon multiple devices” and that “[t]he invention provides for multiple devices to respond as authorized members of a security web such that each device acts as a co-monitoring device within the web” (see Col. 2, lines 37-41; and Figures 1-4 – emphasis added). Lunsford further teaches that “[e]ach device periodically polls for the presence of all the other devices in the piconet and if the signal from any device is not detected by any other device in the piconet then all devices sound an alarm” (Col. 8, lines 42-45 – emphasis added). Thus, because Lunsford clearly teaches multiple devices where each device polls all other devices, the devices in Lunsford are clearly registered with other devices.

Therefore, since Doub discloses a device that is only registered with a single control unit, and the control unit of Doub would be inoperable to control the device if the device were registered to more than one control unit, as admitted by the Examiner, it is clear that modifying the device of Doub according to the system of Lunsford, in which a device is registered with multiple other devices, would render the invention of Doub unsatisfactory for its intended purpose. To emphasize, because the Examiner has admitted that “Doub’s control unit would be inoperable to control the device if the device were...registered with other control units seeking to control the device” (emphasis added), and Lunsford teaches multiple devices polling other devices, the Examiner’s proposed combination of the Doub and Lunsford reference is improper under *In re Gordon*.

Additionally, appellant respectfully asserts that the third element of the *prima facie* case of obviousness has also not been met by the prior art excerpts relied on by the Examiner. For example, with respect to independent Claim 29, the Examiner has relied on Col. 7, lines 9-15; and Col. 8 lines 38-49 from Lunsford to make a prior art showing of appellant’s claimed technique “wherein the control unit includes a control unit display, the control unit display being configured to display information associated with the device when it is determined that the device is not within the range of communications of the control unit.”

Appellant respectfully asserts that Col. 7, lines 9-15 from Lunsford, as relied on by the Examiner, merely teaches that “upon the determination of a non-authorized loss of proximity, an event is initiated upon at least one device in the security web” and that “[t]he event initiated may

vary widely with examples being the activation of audio and visual alarms, the activation and deactivation of user pre-determined devices, and the transmission of communications to a device outside of the security web” (Col. 7, lines 9-15 – emphasis added).

However, only generally disclosing that visual alarms may be initiated upon the loss of proximity of a device, as in Lunsford, in no way specifically suggests that “the control unit includes a control unit display, the control unit display being configured to display information associated with the device when it is determined that the device is not within the range of communications of the control unit” (emphasis added), as claimed by appellant. Simply indicating that a visual alarm may be initiated, as in Lunsford, simply fails to meet “display[ing] information associated with the device” via “a control unit display” (emphasis added), as claimed by appellant.

Additionally, Col. 8, lines 45-49 from Lunsford, as relied on by the Examiner, simply teaches that “any device which loses contact with all other devices of the piconet displays the owners name, address, and telephone number and then locks itself from further use until such time as a password is entered into the device” (emphasis added).

However, displaying the owner’s name, address, and telephone number on the device which has lost contact with all other devices, as in Lunsford, in no way suggests that “the control unit includes a control unit display, the control unit display being configured to display information associated with the device when it is determined that the device is not within the range of communications of the control unit” (emphasis added), as claimed by appellant. Clearly, displaying the owner’s information on the device which has lost contact, as in Lunsford, fails to suggest “display[ing] information associated with the device” via “a control unit display” (emphasis added), as claimed by appellant.

In addition, with respect to independent Claim 29, the Examiner has again relied on Col. 7, lines 9-15 and Col. 8, lines 38-49 in Lunsford to make a prior art showing of appellant’s claimed technique “wherein the device includes a device display, the device display being configured to display information associated with the control unit when it is determined that the device is not within the range of communications of the control unit.”

Appellant respectfully asserts that, as argued above, the excerpts relied on by the Examiner only generally disclose that visual alarms may be initiated upon the loss of proximity of a device and that the owner's name, address, and telephone number are displayed on the device which has lost contact with all other devices. Clearly, only generally disclosing visual alarms, along with displaying information on the device which has lost contact with all other devices, as in Lunsford, fails to meet appellant's claimed technique "wherein the device includes a device display, the device display being configured to display information associated with the control unit when it is determined that the device is not within the range of communications of the control unit" (emphasis added), as claimed.

Further, with respect to independent Claim 29, the Examiner has relied on Col. 2, lines 30-63; and Col. 6, lines 41-53 from Logan to make a prior art showing of appellant's claimed technique "wherein the device is configured to periodically send the identifying signal utilizing a period of time which is configured based on movements of an owner."

Appellant respectfully asserts that the excerpts relied on by the Examiner merely teach that "Blue Tooth chips could be integrated into a small device (here called a 'badge') whose prime function is to indicate position and which can be...placed on or near stationary devices, such as the Palm docking station, or the cell phone recharger, with which Bluetooth devices or things bearing other Bluetooth badges could link to at times" (Col. 6, lines 47-53 - emphasis added). In addition, the excerpts relied on by the Examiner teach that "[a]lthough the Bluetooth chips in these devices may be primarily intended for different functions, they can play a useful role in the position monitoring and notification system contemplated by the present invention" (Col. 2, lines 59-62 - emphasis added).

However, using Blue Tooth chips to indicate position and for position monitoring, as in Logan, fails to even suggest "a period of time which is configured based on movements of an owner," let alone that "the device is configured to periodically send the identifying signal utilizing a period of time which is configured based on movements of an owner" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

## VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A handheld security system, comprising:
  - a Bluetooth-enabled control unit having a range of communications; and
  - a Bluetooth-enabled device, wherein the device is registered with the control unit such that the device cooperates with the control unit using Bluetooth communications to determine when the device is within the range of communications of the control unit, wherein when it is determined that the device is within the range of communications of the control unit, the device is functional, and when it is determined that the device is not within the range of communications of the control unit, the device is at least partially non-functional;
    - wherein the device is configured to periodically send an identifying signal to the control unit and the control unit is configured to send a return signal to the device when the identifying signal is received by the control unit;
    - wherein when the device is at least partially non-functional in a situation where it is determined that the device is not within the range of communications of the control unit, the device is configured to continue periodically sending the identifying signal to the control unit;
    - wherein the control unit is configured to produce an alert when it is determined that the device is not within the range of communications of the control unit;
    - wherein the control unit includes a control unit display, the control unit display being configured to display information associated with the device when it is determined that the device is not within the range of communications of the control unit;
    - wherein the device includes a device display, the device display being configured to display information associated with the control unit when it is determined that the device is not within the range of communications of the control unit;
    - wherein the device is configured to periodically send the identifying signal utilizing a period of time which is configured based on movements of an owner.
2. (Cancelled)

3. (Previously Presented) The handheld security system according to claim 1 wherein the device includes a lockout interface, wherein when the device does not receive the return signal in response to the identifying signal, the device is not within the range of communications of the control unit and the lockout interface locks out the device and causes the device to be at least partially non-functional.
4. (Cancelled)
5. (Previously Presented) The handheld security system according to claim 3 wherein when the device receives the return signal, the lockout interface unlocks the device and causes the device to be functional.
6. (Original) The handheld security system according to claim 1 wherein the device is exclusively registered with the control unit.
7. (Cancelled)
8. (Cancelled)
9. (Cancelled)
10. (Previously Presented) A method for executing a security protocol for a first Bluetooth-enabled device with respect to a second Bluetooth-enabled device, the method comprising:
  - periodically emitting a first Bluetooth transmission signal from the first Bluetooth-enabled device;
  - determining if a second Bluetooth transmission signal is received from the second Bluetooth-enabled device; and
  - locking out the first Bluetooth-enabled device to at least partially prevent the first Bluetooth-enabled device from functioning if it is determined that the second Bluetooth transmission signal is not received, wherein the first Bluetooth-enabled device periodically emits the first Bluetooth transmission signal while being locked out in a situation where it is determined that the second Bluetooth transmission signal is not received;

wherein the second Bluetooth-enabled device is configured to produce an alert when it is determined that the second Bluetooth transmission signal is not received;

wherein the second Bluetooth-enabled device includes a second Bluetooth-enabled device display, the second Bluetooth-enabled device display being configured to display information associated with the first Bluetooth-enabled device when the first Bluetooth-enabled device is locked out;

wherein the first Bluetooth-enabled device includes a first Bluetooth-enabled device display, the first Bluetooth-enabled device display being configured to display information associated with the second Bluetooth-enabled device when the first Bluetooth-enabled device is locked out;

wherein the first Bluetooth-enabled device is configured to periodically emit the first Bluetooth transmission signal utilizing a period of time which is configured based on movements of an owner.

11. (Cancelled)

12. (Cancelled)

13. (Cancelled)

14. (Previously Presented) The method as recited in claim 10 wherein locking out the first Bluetooth-enabled device includes:

displaying information on the first Bluetooth-enabled device display of the first Bluetooth-enabled device which indicates that the first Bluetooth-enabled device is locked out.

15. (Original) The method as recited in claim 10 further including:

operating the first Bluetooth-enabled device if it is determined that the second Bluetooth transmission signal is received.

16. (Previously Presented) A method for executing a security protocol with respect to at least a first Bluetooth-enabled device and a second Bluetooth-enabled device, the method comprising:

determining when a first Bluetooth transmission signal is received from the second Bluetooth-enabled device, wherein the second Bluetooth-enabled device automatically and periodically emits the first Bluetooth transmission signal;

emitting a second Bluetooth transmission signal when it is determined that the first Bluetooth transmission signal is received from the second Bluetooth-enabled device; and

generating an alarm to indicate that the second Bluetooth-enabled device is not within a communications range of the first Bluetooth-enabled device when it is determined that the first Bluetooth transmission signal is not received from the second Bluetooth-enabled device;

wherein after the generation of the alarm, the second Bluetooth-enabled device is configured to continue periodically emit the first Bluetooth transmission signal to the first Bluetooth-enabled device in a situation where it is determined that the first Bluetooth-enabled device is not within the range of communications of the second Bluetooth-enabled device;

wherein the second Bluetooth-enabled device includes a second Bluetooth-enabled device display, the second Bluetooth-enabled device display being configured to display information associated with the first Bluetooth-enabled device when it is determined that the first Bluetooth-enabled device is not within the range of communications of the second Bluetooth-enabled device;

wherein the first Bluetooth-enabled device includes a first Bluetooth-enabled device display, the first Bluetooth-enabled device display being configured to display information associated with the second Bluetooth-enabled device when it is determined that the first Bluetooth-enabled device is not within the range of communications of the second Bluetooth-enabled device;

wherein the second Bluetooth-enabled device is configured to periodically emit the first Bluetooth transmission signal utilizing a period of time which is configured based on movements of an owner.

17. (Cancelled)

18. (Cancelled)

19. (Original) The method as recited in claim 16 wherein determining when the first Bluetooth transmission signal is received from the second Bluetooth-enabled device includes:



determining when the second Bluetooth-enabled device is registered with the first Bluetooth-enabled device, wherein emitting the second Bluetooth transmission signal when it is determined that the first Bluetooth transmission signal is received from the second Bluetooth-enabled device includes emitting the second Bluetooth transmission signal when it is determined that the second Bluetooth-enabled device is registered with the first Bluetooth-enabled device.

20. (Previously Presented) A first device comprising:

a Bluetooth-enabled mechanism;

computer code that causes the Bluetooth-enabled mechanism to periodically emit a first Bluetooth transmission signal;

computer code that causes the Bluetooth-enabled mechanism to receive a second Bluetooth transmission signal from a second Bluetooth-enabled device;

computer code for determining when the second Bluetooth transmission signal is received;

computer code for locking out the first device to at least partially prevent the first device from being operational when it is determined that the second Bluetooth transmission signal is not received;

wherein the Bluetooth-enabled mechanism periodically emits the first Bluetooth transmission signal while the first device is locked out in a situation where it is determined that the second Bluetooth transmission signal is not received;

a processor for executing the computer codes; and

a computer-readable medium that stores the computer codes;

wherein the second Bluetooth-enabled device is configured to produce an alert when it is determined that the second Bluetooth transmission signal is not received;

wherein the second Bluetooth-enabled device includes a second Bluetooth-enabled device display, the second Bluetooth-enabled device display being configured to display information associated with the first device when the first device is locked out;

wherein the first device includes a first device display, the first device display being configured to display information associated with the second Bluetooth-enabled device when the first device is locked out;

wherein the Bluetooth-enabled mechanism is configured to periodically emit the first Bluetooth transmission signal utilizing a period of time which is configured based on movements of an owner.

21. (Cancelled)

22. (Cancelled)

23. (Cancelled)

24. (Previously Presented) The first device according to claim 20 wherein the computer code for locking out the first device includes computer code for displaying information on the first device display to indicate that the first device is locked out when it is determined that the second Bluetooth transmission signal is not received.

25. (Original) The first device according to claim 20 wherein the Bluetooth-enabled mechanism is a Bluetooth-enabled radio.

26. (Previously Presented) A first device comprising:

a Bluetooth-enabled mechanism, the Bluetooth-enabled mechanism being configured to receive a first Bluetooth transmission signal from a second device that periodically emits the first Bluetooth transmission signal;

computer code for determining when a first Bluetooth transmission signal is received;

computer code for causing the Bluetooth-enabled mechanism to emit a second Bluetooth transmission signal when it is determined that the first Bluetooth transmission signal is received;

computer code for generating an alarm to indicate that the second device is not within a communications range of the first device when it is determined that the first Bluetooth transmission signal is not received;

wherein after the generation of the alarm, the second device is configured to continue periodically emitting the first Bluetooth transmission signal in a situation where it is determined that the first device is not within the range of communications of the second device;

a processor that executes the computer codes; and

a computer-readable medium that stores the computer codes;

wherein the second device includes a second device display, the second device display being configured to display information associated with the first device when it is determined that the first device is not within the range of communications of the second device;

wherein the first device includes a first device display, the first device display being configured to display information associated with the second device when it is determined that the first device is not within the range of communications of the second device;

wherein the second device is configured to periodically emit the first Bluetooth transmission signal utilizing a period of time configured which is based on movements of an owner.

27. (Cancelled)

28. (Cancelled)

29. (Previously Presented) A handheld security system, comprising:

a WiFi-enabled control unit having a range of communications; and

a WiFi-enabled device, wherein the device is registered with the control unit such that the device cooperates with the control unit using WiFi communications to determine when the device is within the range of communications of the control unit, wherein when it is determined that the device is within the range of communications of the control unit, the device is functional, and when it is determined that the device is not within the range of communications of the control unit, the device is at least partially non-functional;

wherein the device is configured to periodically send an identifying signal to the control unit and the control unit is configured to send a return signal to the device when the identifying signal is received by the control unit;

wherein when the device is at least partially non-functional in a situation where it is determined that the device is not within the range of communications of the control unit, the device is configured to continue periodically sending the identifying signal to the control unit;

wherein the control unit is configured to produce an alert when it is determined that the device is not within the range of communications of the control unit;

wherein the control unit includes a control unit display, the control unit display being configured to display information associated with the device when it is determined that the device is not within the range of communications of the control unit;

wherein the device includes a device display, the device display being configured to display information associated with the control unit when it is determined that the device is not within the range of communications of the control unit;

wherein the device is configured to periodically send the identifying signal utilizing a period of time which is configured based on movements of an owner.

30. (Cancelled)

31. (Previously Presented) The handheld security system according to claim 29 wherein the device includes a lockout interface, wherein when the device does not receive the return signal in response to the identifying signal, the device is not within the range of communications of the control unit and the lockout interface locks out the device and causes the device to be at least partially non-functional.

32. (Cancelled)

33. (Previously Presented) The handheld security system according to claim 31 wherein when the device receives the return signal, the lockout interface unlocks the device and causes the device to be functional.

34. (Previously Presented) The handheld security system according to claim 1 wherein the device display is configured to display a message that warns that the device is at least one of lost and stolen, when the device is at least partially non-functional.

35. (Previously Presented) The handheld security system according to claim 1 wherein the device display is configured to display contact information that is capable of being used by someone who locates the device to identify the owner of the device, when the device is at least partially non-functional.

36. (Previously Presented) The handheld security system according to claim 1 wherein the device is configured to periodically send the identifying signal utilizing the period of time of at least one hour for accommodating the owner who rarely leaves a particular area.
37. (Previously Presented) The handheld security system according to claim 1 wherein the device is configured to periodically send the identifying signal utilizing the period of time of less than 15 minutes for accommodating the owner who travels frequently.
38. (Previously Presented) The handheld security system according to claim 1 wherein the device is configured to periodically send the identifying signal as long as the device has access to power.

**IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))**

There is no such evidence.

**X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))**

Since no decision(s) has been rendered in such proceeding(s), no material is included in this Related Proceedings Appendix.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NA11P312).

Respectfully submitted,

By: /KEVINZILKA/  
Kevin J. Zilka  
Reg. No. 41,429

Date: June 28, 2007

Zilka-Kotab, P.C.  
P.O. Box 721120  
San Jose, California 95172-1120  
Telephone: (408) 971-2573  
Facsimile: (408) 971-4660